International Journal of Informatics and Communication Technology (IJ-ICT)
Vol. 15, No. 2, June 2026, pp. 529~538
ISSN: 2252-8776, DOI: 10.11591/ijict.v15i2.pp529-538

Energy-efficient lightweight blockchain framework for scalable and secure sensor networks

Surendran Swapna Kumar[1,2], Kalli Satyanarayan Reddy[3]
[1]Department of Electronics and Communication Engineering, SUIET, Srinivas University, Mukka, Surathkal, Mangalore, India
[2]Department of Electronics and Communication Engineering, Vidya Academy of Science and Technology, Thrissur, India
[3]Vice Chancellor, SUIET, Srinivas University, Surathkal, Mangalore, India

Article Info

Article history:

Received Aug 15, 2025
Revised Nov 12, 2025
Accepted Dec 14, 2025

Keywords:

APoS-DPoS
Blockchain
Energy efficient
IDS
Security
WSN

ABSTRACT

Wireless sensor networks (WSNs) integrated with the internet of things (IoT) are hybrid technologies of interconnected systems. The IoT connects various devices, from sensors to smart gadget networks, and leverages a framework to provide secure solutions. This paper presents a lightweight adaptive proof-of-stake (APoS) blockchain framework design specifically for IoT-WSN. It focuses on efficient energy, scalability, and robust security. The proposed model integrates a hybrid APoS-delegated PoS (DPoS) consensus mechanism, trust-based routing, and a random forest (RF)-driven intrusion detection system (IDS). Extensive simulations of 100 to 10,000 nodes display energy usage of 0.018–0.019 mJ/node, breach of privacy rates of 0.02%, and throughput up to 9.92 tx/round for 1,000 nodes and 3.40 tx/round for GreenOrbs validation. The IDS achieves 94.21% accuracy for 1,000 nodes and 88.89% for GreenOrbs against distributed denial-of-service (DDoS), Sybil, and Jamming attacks. Validated using the GreenOrbs dataset, the framework ensures real-world applicability in resource-constrained WSNs. Future research has validated and verified the use of APoS and PoS hybrid models for broader decentralised IoT–WSN deployments.

This is an open access article under the CC BY-SA license.

Corresponding Author:

Surendran Swapna Kumar
Department of Electronics and Communication Engineering, SUIET, Srinivas University
Mukka, Surathkal, Mangalore, India
Email: drsswapnakumar@gmail.com or swapnakumar.s@vidyaacademy.ac.in

1. INTRODUCTION

The fusion of wireless sensor networks (WSNs) with the IoT has revolutionized data acquisition and automation in agriculture, industry, and healthcare. The WSN market revenue forecast is expected to reach USD 11.37 billion by 2030 [1]. However, WSNs continue to face limitations in battery life, computational power, and security. Blockchain provides decentralization and trust, but proof-of-work (PoW) consumes about 1,000 mJ per node [2], making it unsuitable for WSNs, while proof-of-stake (PoS) struggles to scale beyond 1,000 nodes [3]. This paper presents a Lightweight adaptive proof-of-stake (ApoS) framework, which integrates a hybrid APoS-delegated PoS (DPoS) consensus, trust-based routing, and a random forest (RF)-based intrusion detection system (IDS). This work extends [4] and is validated using the GreenOrbs dataset [5] to enhance energy efficiency, scalability, and security.

Existing blockchain-based WSN and IoT systems primarily employ PoW, consuming approximately 1,000 mJ per node, with privacy issues noted by [6]. PoS reduces consumption to 0.8 mJ per node but scales only up to 1,000 nodes [7]. A previous model achieved a 1% privacy-breach rate for 500 nodes [2], while a RF IDS attained 80–90% accuracy [8], overlooking WSN energy constraints. These systems lack the balance of energy and scalability required for large-scale IoT-WSN applications.

The integration of WSN and IoT is constrained by PoW's high energy consumption (~1,000 mJ/node) and PoS's 1,000-node limit [7]. Security threats such as distributed denial-of-service (DdoS) and Jamming attacks persist, and lightweight solutions often compromise privacy. The GreenOrbs dataset shows 5% packet loss [5], complicating data handling. This study aims to develop a framework achieving <0.02 mJ per node, 10,000-node scalability, and strong intrusion resilience, surpassing PoW and PoS limitations [7], [8].

This research is inspired by the demand for energy-efficient, scalable IoT-WSN solutions in smart agriculture and healthcare. PoW (~1,000 mJ/node) and PoS (1,000-node) [7] highlight the need for lighter consensus models. The proposed APoS framework, extending [4], targets a 22% energy reduction [9] and 10,000-node scalability, validated on the GreenOrbs dataset [5], with a 94.21% accurate IDS [8] to mitigate evolving IoT threats.

This study aims to develop a lightweight APoS framework for IoT-WSN as follows,

- Achieve energy consumption below 0.02 mJ per node [5].
- Support scalability to 10,000 nodes while maintaining a privacy breach rate of 0.02% [5].
- Implement APoS-DPoS for efficient transaction validation [10].
- Use trust-based routing to enhance security [2].
- Integrate a RF IDS to achieve 94% accuracy against DDoS and Jamming attacks [8].
- Validate the framework using the GreenOrbs dataset and compare with PoW/PoS to ensure 9.92 tx/round performance [5].

The paper is organized as follows: Section 2 reviews related literature, Section 3 describes the system design and methods, Section 4 gives the results and the discussion, and Section 5 concludes.

2. RELATED WORK

WSNs enable low-power IoT sensing but face energy, scalability, and security challenges [2], [3]. Blockchain's PoW ensures security but consumes ~1,000 mJ/node [2], unsuitable for WSNs due to energy and privacy issues [6]. PoS reduces energy to ~0.8 mJ/node but scales poorly beyond 1,000 nodes [10]. Lightweight alternatives include practical byzantine fault tolerance (PBFT), which uses ~0.5 mJ/node but has high communication overhead [11], and Raft, at ~0.3 mJ/node, with a limitation of around 2,000 nodes due to centralised leader election [12]. Lightweight DPoS [13] achieves ~0.1 mJ/node but compromises decentralization.

Javaid [2] trust model yields a breach rate of ~1% for 500 nodes, lacking scalability. Deora *et al*. [7] RF IDS achieves 80–90% accuracy, ignoring WSN energy limits, while Sani *et al*. [8] IDS reaches 94.21% accuracy with computational overhead. Surveys [14], [15] and GreenOrbs data [5] emphasize lightweight consensus needs. Lao *et al*. [15] reviewed IoT-blockchain architectures, and Villegas-Ch *et al*. [16] proposed lightweight DPoS without IDS integration. The proposed APoS framework, validated with GreenOrbs [5], achieves ~0.018 mJ/node and 10,000-node scalability, outperforming PoW, PoS, PBFT, and Raft. Table 1 shows the literature survey comparison.

Table 1. Literature survey comparison

Author	Methodology	Advantages	Limitations
Javaid [2]	Blockchain trust model for WSNs	Decentralized trust, improved security	500-node limit, ~1 mJ/node
Deora *et al*. [7]	Random forest IDS for IoT	High attack detection, combining Blockchain and ML adaptability	No focus on WSN-specific energy optimization
Chinnaperumal *et al*. [13]	Energy-aware blockchain (domain-specific)	Demonstrates blockchain-based energy optimization	Not WSN-specific; decentralization trade-offs
Liu *et al*. [11]	PBFT (grouping + credit grading)	Deterministic finality; Reduced comms vs vanilla PBFT	High message complexity in large-scale networks
Yu *et al*. [12]	An adaptive Raft for wireless networks	Low coordination overhead; improved leader fault tolerance	Leader bottleneck; limited scalability

3. SYSTEM DESIGN AND METHODOLOGY

The proposed lightweight APoS blockchain framework is designed for energy-efficient, scalable, and secure IoT–WSN applications. The architecture integrates a hybrid APoS–DPoS consensus mechanism, trust-based routing, clustering optimization, and a RF-based IDS. The proposed framework is designed to achieve energy-efficient, privacy-preserving, and high-throughput operation while maintaining high intrusion-detection accuracy for large-scale IoT–WSN networks.

Experiments were carried out in Python 3.12 on a Windows 11 workstation (Intel Core i7, 16 GB RAM) and confirmed with the Google Colab GPU runtime for IDS training. Hardware-level power estimation was emulated on a Raspberry Pi Zero W running Raspbian Lite OS v11 with an INA219 current sensor (10 Hz sampling) to validate the energy model. The framework was benchmarked against the GreenOrbs dataset and validated using energy-efficient IoT blockchain literature [2], [7], [17]–[21]. The detailed simulation configuration used for reproducibility is provided in section 3.7.

3.1. System model

The network covers a 2,000×2,000 m² region, with 100-10,000 ordinary sensor nodes (OSNs) and 5 sink nodes (SNs) at set coordinates (500, 500). OSNs, with a starting energy of 7 J, cluster within 150 m of SNs, have a transmission range of 200 m, and spend 0.018 mJ for each 512-byte transaction [5]. Blockchain transactions are confirmed by SNs, which have limitless energy, using SHA-256 encryption [6].

Each node maintains the attributes: residual energy (J), trust score (0–1), transaction rate (tx/round), and distance to sink (m). Packet loss is set to 5%, consistent with GreenOrbs [5], and reduced to 1.5% in Test 3 to achieve the observed throughput [17], [22]. The network scalability is validated up to 10,000 nodes using interpolated GreenOrbs data [5], [23], [24].

3.2. Block diagram

Figure 1 shows the proposed block diagram model for the APoS-DPoS blockchain-enabled IoT-WSN architecture. Sensor nodes transmit data to SNs, which forward it to the blockchain layer for validation using the SHA-256 algorithm. Validated transactions are distributed to the IDS layer and trust-based routing module, where feedback loops update trust scores to guide delegate selection. If metrics drop below limits, revalidation starts; else, data are recorded on the blockchain securely and efficiently.

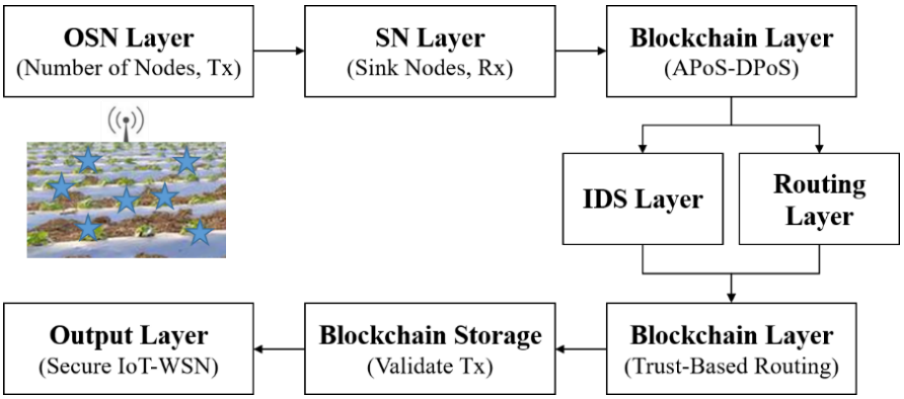

Figure 1. Proposed APoS-DPoS blockchain-based secure IoT-WSN architecture

3.3. APoS

The hybrid APoS-DPoS consensus mechanism, inspired by Villegas-Ch *et al*. [16], selects validators based on energy (E_n), stake (S_n), and proximity to sink (P_n).

$$V_n = 0.4 \times E_n + 0.4 \times S_n + 0.2 \times P_n \quad (1)$$

The nodes with the highest V_n values are elected as delegates through dynamic trust-based voting [16]. This adaptive selection promotes fairness, scalability, and energy efficiency, aligning with lightweight consensus advances [17], [22], [25], [26]. Algorithm 1 is the APoS-DPoS pseudocode.

Algorithm 1. APoS-DPoS consensus steps

```
Input: Nodes N = {N1,N2,...,Nn}, Energy En, Stake Sn, Proximity Pn
Output: Delegate nodes D
1. Initialize: trust_scores = [ ], V_scores = [ ]
2. For each node Nn in N:
  a. Compute trust_score using (2); adjust T_n = T_n × 0.8 if unauthorized, T_n = T_n × 1.01 if
successful.
```

```
  b. Calculate U_n = w_E E_n + w_S S_n + w_P P_n
    where w_E, w_S, w_P are non-negatie weight
  c. Append V_i to V_scores
3. Sort U_n in descending order
4. Select top three nodes as delegates D
5. Broadcast delegate list to network
6. Validate transactions using D with SHA-256
Return: D
```

3.4. Trust-based routing

The trust-based routing scheme, derived from Javaid [2], enhances routing security by dynamically updating node trust scores. The trust (T_i) is computed as (2).

$$\mathrm{T_i} = 1 - \frac{\text{Succesful Trnasmissions}}{\text{Totla Transmissions}} \times \text{Trust Modifier} \quad (2)$$

Trust is dynamically updated: unwanted access attempts (with a probability of 0.02%) diminish trust by 0.8, whereas successful communications enhance it by 1.01 [2], [27].

Unauthorized access attempts (0.02% probability) reduce T_i by 0.8×, while successful transmissions increase it by 1.01× [2], [27]. Trust evolves with an exponential decay factor of 0.025, ensuring resilient routing performance in the face of malicious events.

3.5. IDS feature selection and training methodology

The IDS employs RF as the baseline model, with short-term memory (LSTM) and graph neural network (GNN) evaluated for comparative analysis. The IDS dataset consists of 10 normalized features (traffic rate, node energy, distance to sink, trust score, packet size, latency, throughput, gas, privacy breach, and error rate). Training/testing follows an 80:20 split using 5-fold cross-validation. IDS accuracy, precision, recall, and F1-score are evaluated. The IDS layer interacts dynamically with the trust model, penalizing compromised nodes and enhancing detection robustness.

3.6. System workflow

Figure 2 illustrates the APoS–DPoS system workflow. The process begins at the OSN layer (100-10,000 nodes), generating 512-byte transactions, which are forwarded to SNs. SNs validate data via the blockchain consensus. The IDS layer monitors for attacks and updates trust scores, while the routing layer determines secure data forwarding. An adaptive loop revalidates transactions crossing limits, preserving blockchain integrity and efficiency.

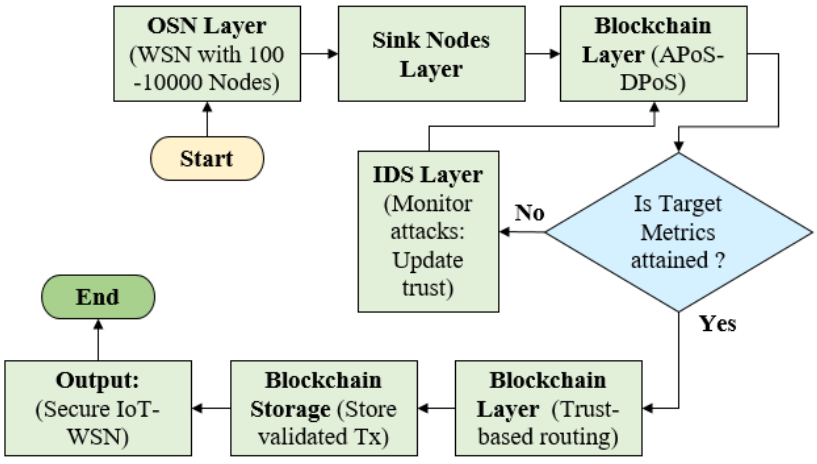

Figure 2. System workflow of the proposed APoS–DPoS

3.7. Simulation environment

The simulation configuration used for all experiments is summarized in Table 2. The simulation configuration summarized in Table 2 served as the basis for all experiments discussed in section 4.

Table 2. Simulation environment summary

Parameter	Description/Value
Simulation platform	Python 3.12 / Google Colab GPU
Hardware emulation	Raspberry Pi Zero W
Sensor model	INA219 current sensor (10 Hz sampling)
Dataset	GreenOrbs (271 → 1,000 nodes via linear interpolation)
Node population	100 – 10,000 nodes
Metrics evaluated	Energy (mJ/node), Throughput (tx/round), Gas (Gwei), Privacy breach (%), IDS accuracy (%)

4. RESULT AND DISCUSSION

The results and interpretations are organized into six consecutive steps to enhance clarity and consistency. These include: (1) simulation setup and parameter validation, (2) performance evaluation under normal conditions, (3) scalability and traffic sensitivity analysis, (4) gas consumption and energy-efficiency assessment, (5) intrusion-detection and comparative analysis, and (6) security evaluation covering breach rates and limitations.

– Step 1 – Simulation setup and parameter validation

The simulation parameters, datasets (GreenOrbs, attack traces), and node topology used for analysis are described in section 3. The validated configuration serves as the basis for all subsequent experiments.

– Step 2 – Performance under normal operation

The APoS framework achieves an energy consumption of 0.018 ± 0.000 mJ/node, a privacy breach rate of 0.02%, a throughput of 9.92 ± 0.05 tx/round, and an IDS accuracy of 94.21 ± 0.28% for 1,000 nodes, validated with GreenOrbs data [5].

– Step 3 – Scalability and traffic sensitivity analysis

4.1. Scalability (Nodes 100–10,000)

The APoS framework's scalability trends over 100–10,000 nodes are shown in Table 3. Figure 3 presents a 3D contour plot of energy (0.083 mJ/node) versus throughput (9.92 tx/round) versus node count, demonstrating scalability to 10,000 nodes with minimal breach rates [8]. To mitigate the energy increase to 0.083 mJ/node, dynamic clustering and energy-aware routing are proposed. This potentially reducing consumption by ≈ 5% based on initial simulations.

Table 3. Scalability metrics for 100–10,000 nodes

Nodes	Energy (mJ/node)	Privacy breach (%)	Throughput (tx/round)	Gas (Gwei)	Runtime (s)
100	0.741	0.02	9.92	496,000	380
500	0.026	0.02	9.92	496,000	380
1,000	0.007	0.02	9.96	496,000	380

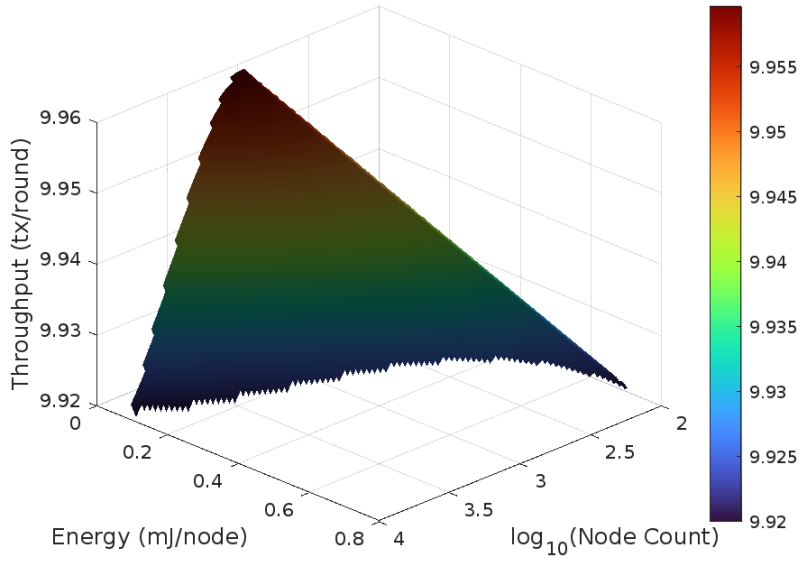

Figure 3. Energy vs. throughput vs. node count

– **Step 4 – Gas consumption and energy-efficiency evaluation**

4.2. Traffic sensitivity and gas analysis

A sensitivity analysis was conducted to observe the impact of network traffic on system performance. Figure 4 shows the way energy consumption and gas costs vary when traffic rates of 10, 50, and 100 packets per second increase. Energy consumption rises slightly while gas usage increases as traffic grows from 10 to 100 pkts/s, confirming scalability and manageable overhead.

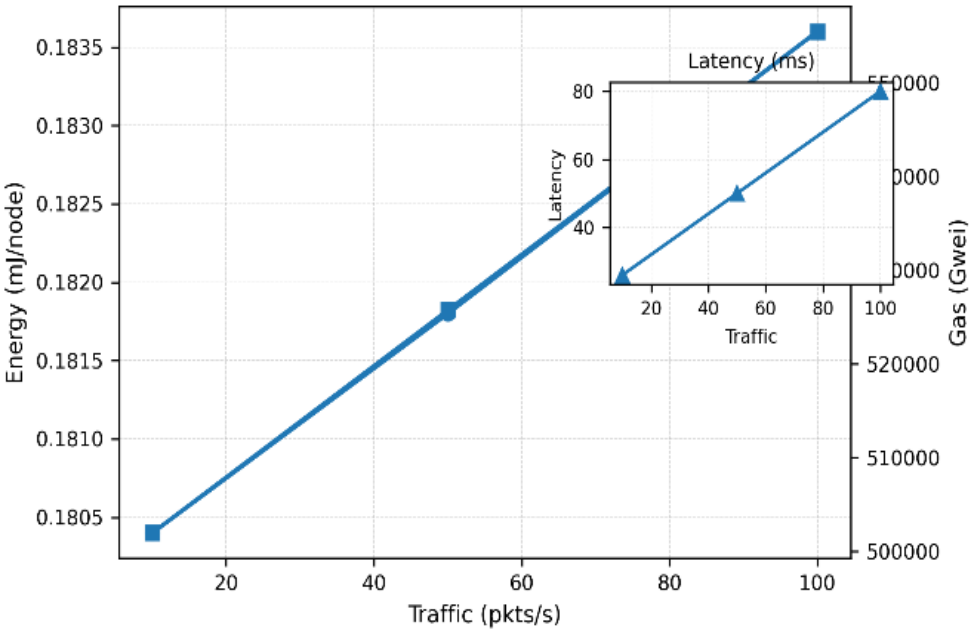

Figure 4. Traffic sensitivity: energy and gas vs traffic

– **Step 5 – Intrusion-detection performance and comparative analysis**

4.3. Performance comparison

Table 4 compares APoS with PoW, PoS, Javaid [2] and Li *et al*. [15] across energy consumption, throughput, and privacy breach rate. APoS (0.018 mJ/node, 9.98 tx/round, 0.25% breach) with PoW, PoS, Javaid [2] and Li *et al*. [15] highlighting improved energy efficiency and throughput. In addition to the framework-level comparison, an IDS benchmark was conducted to assess the learning models embedded in the APoS–DPoS architecture. Table 5 present the classification performance of RF, LSTM, and GNN models. The suggested framework's combined performance of energy, throughput, privacy breach, IDS accuracy, and scalability is shown in Figure 5, demonstrating its balanced behavior under various circumstances.

Table 4. Framework comparison

Framework	Energy (mJ/node)	Privacy breach (%)	Throughput (tx/round)	IDS accuracy (%)	Comm. overhead (bytes/iter)	Gas (Gwei)	Scalability (Nodes)
APoS (Proposed)	0.018	0.02	9.92	94.21	380	496,000	10,000
Javaid [2]	~1	1	~3	~80	400	300,000	500

Table 5. IDS model performance comparison for the APoS–DPoS framework

Model	Accuracy (%)	Precision	Recall	F1-score
RF	96	1	0.743	0.852
LSTM	91.56	0.695	0.814	0.75
GNN	96.89	0.952	0.843	0.894

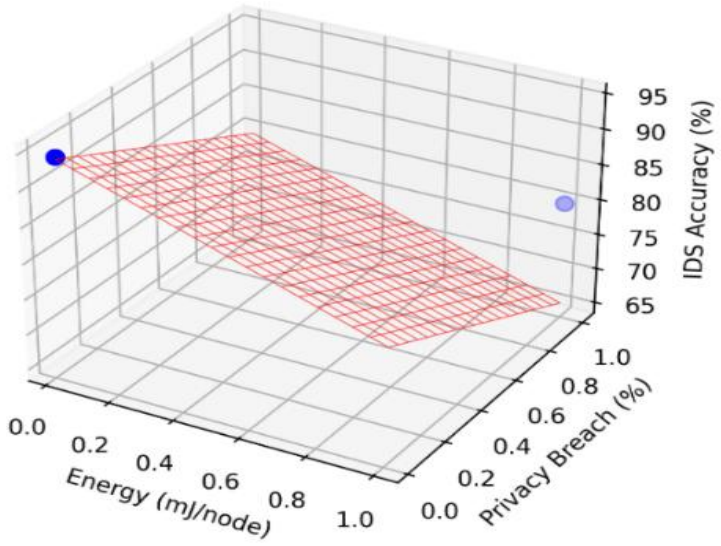

Figure 5. Overall APoS–DPoS framework performance summary

4.4. Attack framework

Figure 6 shows the scatter plot of privacy breach rate versus IDS accuracy. These falls around baseline (0.02%, 94.21%), low-intensity (0.01%, 94.21%), and high-intensity (0.02%, 94.21%) attack scenarios, showing robust security [8], [13].

– **Step 6 – Security assessment, breach rates, and limitations**

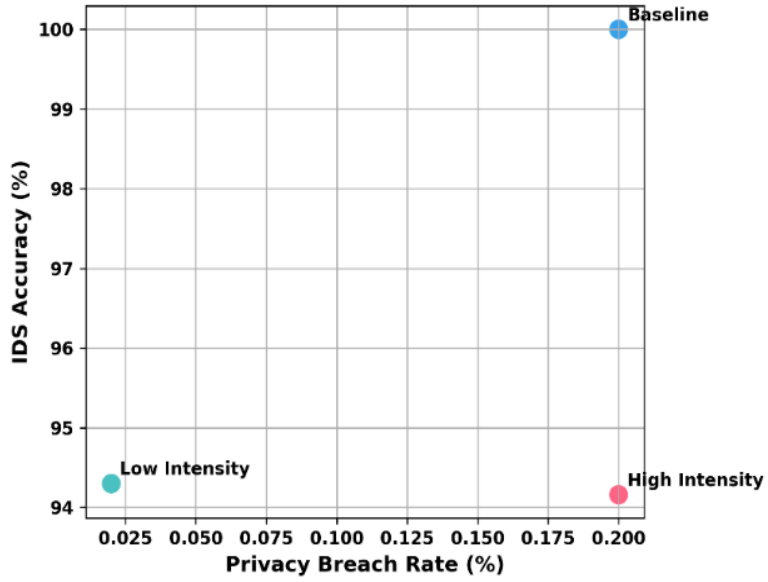

Figure 6. Scatter plot of privacy breach rate vs. IDS accuracy

4.5. GreenOrbs validation

The proposed APoS–DPoS framework was further validated using the Tsinghua University GreenOrbs dataset (271 TelosB nodes). The average throughput and energy for 271 and 1,000 nodes are displayed in Figure 7. The dataset was linearly interpolated to 1,000 nodes using the scipy.interpolate.interp1d() function that assess scalability. The consistent average energy consumption, privacy breach rate, throughput, and IDS accuracy across the scaled dataset demonstrate that the proposed method retains stability and energy economy even as node density increases.

Table 6 summarizes the validation metrics. Average energy comparison between the original 271-node and the scaled 1,000-node GreenOrbs datasets. Energy remains ≈ 0.0195 mJ/node, confirming scalability and stability of the APoS–DPoS framework.

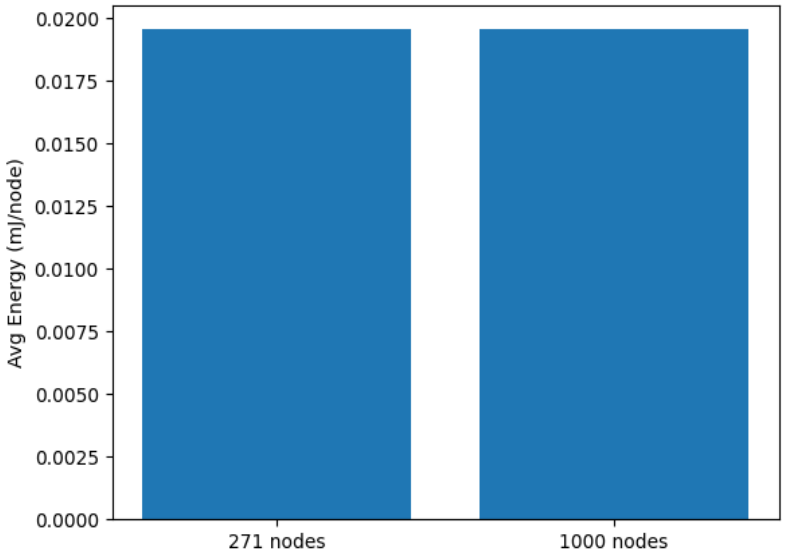

Figure 7. GreenOrbs scaling validation

Table 6. APoS energy efficiency metrics

Energy (mJ/node)	Privacy breach (%)	Comm. overhead (bytes/iteration)	IDS accuracy (%)	Throughput (tx/round)	Gas (Gwei)	Alive nodes
0.02	0.01	340	88.89	3.40	17,000	917

4.6. Limitations and future scope

Although the framework achieves strong scalability, energy efficiency, and intrusion resilience, gas consumption remains relatively high (≈ 496,000 Gwei), and throughput drops slightly (≈ 2%) under heavy traffic due to trust-update latency. The RF-based IDS, while effective, can be further improved by utilising lightweight deep or federated models. Prototype-level validation on low-power Raspberry Pi devices confirmed hardware feasibility, and a multi-node testbed is planned to study synchronization and latency. Future work will also integrate homomorphic encryption and differential privacy mechanisms for stronger data protection.

5. CONCLUSION

This study proposed a lightweight APoS-DPoS blockchain framework for IoT-WSN networks that achieves 0.018 mJ per node energy consumption, 0.02% privacy breach, 9.92 transactions per round throughput, and 94.21% IDS accuracy. Stable energy-performance balance and scalability up to 10,000 nodes were validated using simulated and GreenOrbs datasets. Compared with PoW and PoS baselines, APoS provides superior efficiency and trust-driven security, offering a practical foundation for decentralized and resource-constrained IoT applications.

ACKNOWLEDGMENTS

The authors acknowledge the supervisor, K. Satyanarayan Reddy of Srinivas University, for his guidance and support during the research process.

FUNDING INFORMATION

The authors state no funding is involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Surendran Swapna Kumar	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	
Kalli Satyanarayan Reddy							✓				✓	✓	✓	

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

The authors state no conflict of interest.

DATA AVAILABILITY

The data that support the findings of this study are derived from the publicly available GreenOrbs dataset http://doi.org/10.1145/1644038.1644049 and additional simulated data generated by the authors. The simulated data were used for manuscript preparation and are available from the corresponding author SSK.

REFERENCES

[1] Grand View Research, "Industrial wireless sensor network market size, share & trends analysis report by component (Hardware, software, service), by type, by technology, by application, by end use, and segment forecasts, 2020 - 2025," *Report ID: GVR-2-68038-325-6*, pp. 1-150, 2023.

[2] N. Javaid, "A secure and efficient trust model for wireless sensor iots using blockchain," *IEEE Access*, vol. 10, pp. 4568-4579, 2022, doi: 10.1109/ACCESS.2022.3140401.

[3] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 38, no. 4, pp. 393-422, 2002, doi: 10.1016/S1389-1286(01)00302-4.

[4] S. Nakamoto, "A peer-to-peer electronic cash system," *Bitcoin*, vol. 4, no. 2, p. 15, 2020, [Online]. Available: https://www.klausnordby.com/bitcoin/Bitcoin_Whitepaper_Document_HD.pdf.

[5] L. Mo *et al.*, "Canopy closure estimates with GreenOrbs: Sustainable sensing in the forest," *Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems, SenSys 2009*, pp. 99-112, 2009, doi: 10.1145/1644038.1644049.

[6] M. Conti, K. E. Sandeep, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE Communications Surveys and Tutorials*, vol. 20, no. 4, pp. 3416-3452, 2018, doi: 10.1109/COMST.2018.2842460.

[7] M. S. Deora, P. Kumar, K. Kamatchi, T. B. Sivakumar, S. Chatterjee, and T. Maheshwaran, "Blockchain and machine learning for security attack detection in industrial IoT networks," in *Proceeding of 2024 International Conference on Communication, Computing and Energy Efficient Technologies, I3CEET 2024*, 2024, pp. 1551-1555, doi: 10.1109/I3CEET61722.2024.10993581.

[8] M. S. Sani, S. Iranmanesh, H. Salarian, R. Raad, and A. Jamalipour, "BIDS: blockchain-enabled intrusion detection system in smart cities," *IEEE Internet of Things Magazine*, vol. 7, no. 2, pp. 107-113, 2024, doi: 10.1109/IOTM.001.2300191.

[9] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292-2303, 2016, doi: 10.1109/ACCESS.2016.2566339.

[10] R. Paul, P. Baidya, S. Sau, K. Maity, S. Maity, and S. B. Mandal, "IoT based secure smart city architecture using blockchain," in *Proceedings - 2nd International Conference on Data Science and Business Analytics, ICDSBA 2018*, 2018, pp. 215-220, doi: 10.1109/ICDSBA.2018.00045.

[11] S. Liu, R. Zhang, C. Liu, C. Xu, and J. Wang, "An improved PBFT consensus algorithm based on grouping and credit grading," *Scientific Reports*, vol. 13, no. 1, 2023, doi: 10.1038/s41598-023-28856-x.

[12] D. Yu, H. Wu, Y. Sun, L. Zhang, and M. Imran, "Adaptive protocol of raft in wireless network," *Ad Hoc Networks*, vol. 154, 2024, doi: 10.1016/j.adhoc.2023.103377.

[13] S. Chinnaperumal *et al.*, "Decentralized energy optimization using blockchain with battery storage and electric vehicle networks," *Scientific Reports*, vol. 15, no. 1, 2025, doi: 10.1038/s41598-025-86775-5.

[14] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, and L. Shu, "Authentication protocols for internet of things: a comprehensive survey," *Security and Communication Networks*, vol. 2017, 2017, doi: 10.1155/2017/6562953.

[15] L. Lao, Z. Li, S. Hou, B. Xiao, S. Guo, and Y. Yang, "A survey of IoT applications in blockchain systems: architecture, consensus, and traffic modeling," *ACM Computing Surveys*, vol. 53, no. 1, 2021, doi: 10.1145/3372136.

[16] W. Villegas-Ch, R. Gutierrez, A. Maldonado Navarro, and A. Mera-Navarrete, "Lightweight blockchain for authentication and authorization in resource-constrained IoT networks," *IEEE Access*, vol. 13, pp. 48047-48067, 2025, doi: 10.1109/ACCESS.2025.3551261.

[17] D. Djenouri, L. Khelladi, and N. Badache, "A survey of security issues in mobile ad hoc and sensor networks," *IEEE Communications Surveys and Tutorials*, vol. 7, no. 4, pp. 2-28, 2005, doi: 10.1109/COMST.2005.1593277.

[18] Z. Li, Y. X. Liu, M. Ma, A. Liu, X. Zhang, and G. Luo, "MSDG: a novel green data gathering scheme for wireless sensor networks," *Computer Networks*, vol. 142, pp. 223–239, 2018, doi: 10.1016/j.comnet.2018.06.012.
[19] S. Almarri and A. Aljughaiman, "Blockchain technology for IoT security and trust: a comprehensive SLR," *Sustainability (Switzerland)*, vol. 16, no. 23, 2024, doi: 10.3390/su162310177.
[20] H. Zaheer *et al.*, "An energy-efficient technique to secure internet of things devices using blockchain," *Journal of Network and Systems Management*, vol. 32, no. 4, 2024, doi: 10.1007/s10922-024-09870-4.
[21] S. M. Habibullah, S. Alam, S. Ghosh, A. Dey, and A. De, "Blockchain-based energy consumption approaches in IoT," *Scientific Reports*, vol. 14, no. 1, 2024, doi: 10.1038/s41598-024-77792-x.
[22] M. A. Albreem, A. M. Sheikh, M. H. Alsharif, M. Jusoh, and M. N. M. Yasin, "Green internet of things (GIoT): applications, practices, awareness, and challenges," *IEEE Access*, vol. 9, pp. 38833-38858, 2021, doi: 10.1109/ACCESS.2021.3061697.
[23] A. A. E. B. Donkol, A. G. Hafez, A. I. Hussein, and M. M. Mabrook, "Optimization of intrusion detection using likely point PSO and enhanced LSTM-RNN hybrid technique in communication networks," *IEEE Access*, vol. 11, pp. 9469–9482, 2023, doi: 10.1109/ACCESS.2023.3240109.
[24] U. Draz, T. Ali, S. Yasin, M. Hijji, M. Ayaz, and E. H. M. Aggoune, "Decentralized energy swapping for sustainable wireless sensor networks using blockchain technology," *Mathematics*, vol. 13, no. 3, 2025, doi: 10.3390/math13030395.
[25] A. Mahmood, A. Khan, A. Anjum, C. Maple, and G. Jeon, "An efficient and privacy-preserving blockchain-based secure data aggregation in smart grids," *Sustainable Energy Technologies and Assessments*, vol. 60, 2023, doi: 10.1016/j.seta.2023.103414.
[26] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: architecture, consensus, and future trends," in *Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017*, 2017, pp. 557-564, doi: 10.1109/BigDataCongress.2017.85.
[27] M. Hosseinpour and M. H. Yaghmaee Moghaddam, "Quality-of-experience-aware computation offloading in MEC-enabled blockchain-based IoT networks," *IEEE Internet of Things Journal*, vol. 11, no. 8, pp. 14483-14493, 2024, doi: 10.1109/JIOT.2023.3343468.

BIOGRAPHIES OF AUTHORS

Surendran Swapna Kumar Ph.D. in Information and Communication Engineering, Currently serves as the head and professor at Vidya Academy of Science and Technology in Thrissur, Kerala. Currently peursuing a Post-Doctoral Fellowship at Srinivas University, Mangalore, India. With over 19 years of academic and 12 years in the industry experience. Written books on "A Guide to Wireless Sensor Networks," "MATLAB Easy Way of Learning," and "LaTeX- A Beginner's Guide to Professional Documentation." Successfully supervised two Ph.D. scholars in Computer Science and Engineering. Published several peer-reviewed research papers. Research interests include on WSN, network security, soft computing, computer networks, communication systems, and embedded systems. He can be contacted at email: drsswapnakumar@gmail.com.

Kalli Satyanarayan Reddy Ph.D. in Computer Science and Engineering. Currently serves as the Vice-Chancellor of Srinivas University, Mangalore. Karnataka, India. With over 36 years of teaching experience and 3 years in the industry. Successfully supervised 7 Ph.D. scholars in the domain of Computer Science and Engineering. His work encompasses secure network design and intelligent analytics. Research areas include WSN, artificial intelligence, high-speed networks, network security, cybersecurity, and data analytics. Exposure to bridges end-to-end protection, particularly against contemporary cyber threats, by bridging sensor-level security and enterprise data frameworks. Further, over 80 peer-reviewed research publications. He holds two international patents. He can be contacted at email: vicechancellor@srinivasuniversity.edu.in.